



Where people and technology connect...

Welcome!

Tricks to Combat

Cybercrime!

(Viruses, Trojans and Phishing – OH MY!)



How it works

- Practicing "Safe Internet"
 - What virus protection can and can't do
 - Domain names – how to spot "fake" ones
 - Phishing – guarding your information
 - Viruses/Trojans – how to avoid them



Domain name makeup

- A domain name is an (hopefully) easy to remember name that points to an address on the internet:
 - <http://service.yourcompany.extension>
- It is usually preceded by a "service" word and may be followed by some **page names**
 - <http://www.microsoft.com>
 - <http://download.microsoft.com>

 - <http://download.microsoft.com/servers>



Domain name makeup

- The MOST IMPORTANT PART is what is between the FIRST series of slashes
 - <http://download.microsoft.com/servers/somethingelse>
 - Find the RIGHTMOST "." in the first set of slashes. The words on either side of that "." are the domain name
 - <http://www.anexeon.com/aboutus.html>
 - http://www.usbank.com/cgi_w/cfm/personal/sub_global/usb_internet_banking.cfm



Domain name test – POP QUIZ!

- Identify the domain names

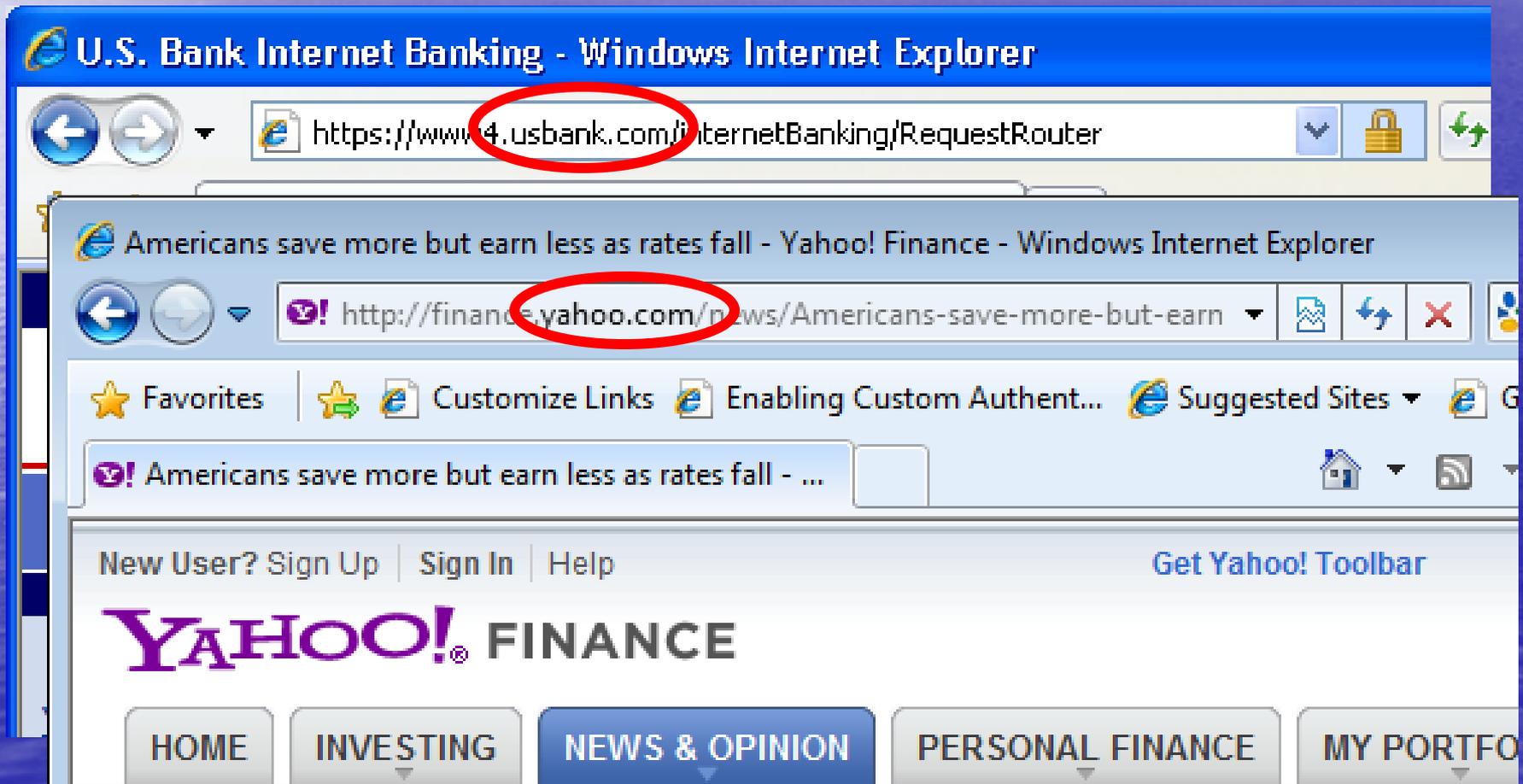
- <http://partners.microsoft.com/login/passupdate.htm>
- <https://customers.wellsfargo.com/password.htm>
- https://www2.customers.citibank.com/personal/sub_global/usb_internet_banking.cfm
- <https://customerservice.usbank.com/customersvc/pass.asp>
- <http://www.nv.gov/MeetingDisplay/CalendarOfMeetings/>



Here's how they fool you!

- Identify the domain names
 - <http://partners.microsoft.com.energytree.ru/passupdt.html>
 - <http://customers.wellsfargo.com.wells-fargo.com/pass.html>
 - http://www2.customers.wellsfargo.com/personal/sub_global/usb_internet_banking.cfm
 - <https://customerservice.usbank.com.usbank.tv/customerservice/passwords.asp>
-

- What is a domain name?





More services

- Anexeon examples of services before the domain name
 - <http://connect.anexeon.com>
 - <http://support.anexeon.com>
 - <http://helpdesk.anexeon.com>
 - <http://cdr.anexeon.com>
 - <http://portal.anexeon.com>
-



Domain Names

- Domain name extensions (top level domains) The Big 7 in the US:
 - .com - commercial
 - .edu - education
 - .gov - government
 - .int – international treaty organizations
 - .mil - military
 - .net – commercial (intended for network infrastructure)
 - .org – non-profit organizations



Country Extensions-

- .AC country-code Ascension Island
- .AD country-code Andorra
- .AE country-code United Arab Emirates
- .AERO sponsored Reserved for members of the air-transport industry
- .AF country-code Afghanistan
- .AG country-code Antigua and Barbuda
- .AI country-code Anguilla
- .AL country-code Albania
- .AM country-code Armenia
- .AN country-code Netherlands Antilles
- .AO country-code Angola
- .AQ country-code Antarctica
- .AR country-code Argentina
- .ASIA sponsored Restricted to the Pan-Asia and Asia Pacific community
- .AT country-code Austria
- .AU country-code Australia
- .au Domain Administration (auDA)
- .AW country-code Aruba
- .AX country-code Aland Islands
- .AZ country-code Azerbaijan
- .BA country-code Bosnia and Herzegovina
- .BB country-code Barbados
- .BD country-code Bangladesh
- .BE country-code Belgium
- .BF country-code Burkina Faso
- .BG country-code Bulgaria
- .BH country-code Bahrain
- .BI country-code Burundi
- .BIZ generic-restricted Restricted for Business
- .BJ country-code Benin
- .BL country-code Saint Barthelemy
- .BM country-code Bermuda
- .BN country-code Brunei Darussalam
- .BO country-code Bolivia
- .BR country-code Brazil
- .BS country-code Bahamas
- .BT country-code Bhutan
- .BV country-code Bouvet Island
- .BW country-code Botswana
- .BY country-code Belarus
- .BZ country-code Belize
- .CA country-code Canada
- .CAT sponsored Reserved for the Catalan linguistic and cultural community
- .CC country-code Cocos (Keeling) Islands
- .CD country-code Congo, The Democratic Republic of the
- .CF country-code Central African Republic
- .CG country-code Congo
- .CH country-code Switzerland
- .CI country-code Cote d'Ivoire
- .CK country-code Cook Islands
- .CL country-code Chile
- .CM country-code Cameroon
- .CN country-code China
- .CO country-code Colombia
- .COM generic Generic top-level domain
- .COOP sponsored Reserved for cooperative associations
- .CR country-code Costa Rica
- .CU country-code Cuba
- .CV country-code Cape Verde
- .CX country-code Christmas Island
- .CY country-code Cyprus
- .CZ country-code Czech Republic



Country Extensions-

- .DE country-code Germany
- .DJ country-code Djibouti
- .DK country-code Denmark
- .DM country-code Dominica
- .DO country-code Dominican Republic
- .DZ country-code Algeria
- .EC country-code Ecuador
- .EDU sponsored Reserved for post-secondary institutions accredited by an agency on the U.S. Department of Education's list of Nationally Recognized Accrediting Agencies
- EDUCAUSE
- .EE country-code Estonia
- .EG country-code Egypt
- .EH country-code Western Sahara
- .ER country-code Eritrea
- .ES country-code Spain
- .ET country-code Ethiopia
- .EU country-code European Union
- .FI country-code Finland
- .FJ country-code Fiji
- .FK country-code Falkland Islands (Malvinas)
- .FM country-code Micronesia, Federated States of
- .FO country-code Faroe Islands
- .FR country-code France
- .GA country-code Gabon
- .GB country-code United Kingdom
- .GD country-code Grenada
- .GE country-code Georgia
- .GF country-code French Guiana
- .GG country-code Guernsey
- .GH country-code Ghana
- .GI country-code Gibraltar
- .GL country-code Greenland
- .GM country-code Gambia
- .GN country-code Guinea
- .GOV sponsored Reserved exclusively for the United States Government
- .GP country-code Guadeloupe
- .GQ country-code Equatorial Guinea
- .GR country-code Greece
- .GS country-code South Georgia and the South Sandwich Islands
- .GT country-code Guatemala
- .GU country-code Guam
- .GW country-code Guinea-Bissau
- .GY country-code Guyana
- .HK country-code Hong Kong
- .HM country-code Heard Island and McDonald Islands
- .HN country-code Honduras
- .HR country-code Croatia
- .HT country-code Haiti
- .HU country-code Hungary
- .ID country-code Indonesia
- .IE country-code Ireland
- .IL country-code Israel
- .IM country-code Isle of Man
- .IN country-code India
- .INFO generic Generic top-level domain



Country Extensions-

- .INT sponsored Used only for registering organizations established by international treaties between governments
- .IO country-code British Indian Ocean Territory
- .IQ country-code Iraq
- .IR country-code Iran, Islamic Republic of
- .IS country-code Iceland
- .IT country-code Italy
- .JE country-code Jersey
- .JM country-code Jamaica
- .JO country-code Jordan
- .JOBS sponsored Reserved for human resource managers
- .JP country-code Japan
- .KE country-code Kenya
- .KG country-code Kyrgyzstan
- .KH country-code Cambodia
- .KI country-code Kiribati
- .KM country-code Comoros
- .KN country-code Saint Kitts and Nevis
- .KP country-code Korea, Democratic People's Republic of
- .KR country-code Korea, Republic of
- .KW country-code Kuwait
- .KY country-code Cayman Islands
- .KZ country-code Kazakhstan
- .LA country-code Lao People's Democratic Republic
- .LB country-code Lebanon
- .LC country-code Saint Lucia
- .LI country-code Liechtenstein
- .LK country-code Sri Lanka
- .LR country-code Liberia
- .LS country-code Lesotho
- .LT country-code Lithuania
- .LU country-code Luxembourg
- .LV country-code Latvia
- .LY country-code Libyan Arab Jamahiriya
- .MA country-code Morocco
- .MC country-code Monaco
- .MD country-code Moldova, Republic of
- .ME country-code Montenegro
- .MF country-code Saint Martin
- .MG country-code Madagascar
- .MH country-code Marshall Islands
- .MIL sponsored Reserved exclusively for the United States Military
- .MK country-code Macedonia, The Former Yugoslav Republic of
- .ML country-code Mali
- .MM country-code Myanmar
- .MN country-code Mongolia
- .MO country-code Macao
- .MOBI sponsored Reserved for consumers and providers of mobile products and services
- .MP country-code Northern Mariana Islands
- .MQ country-code Martinique
- .MR country-code Mauritania
- .MS country-code Montserrat



Country Extensions-

- .MT country-code Malta
- .MU country-code Mauritius
- .MUSEUM sponsored Reserved for museums
- .MV country-code Maldives
- .MW country-code Malawi
- .MX country-code Mexico
- .MY country-code Malaysia
- .MZ country-code Mozambique
- .NA country-code Namibia
- .NAME generic-restricted Reserved for individuals
- .NC country-code New Caledonia
- .NE country-code Niger
- .NET generic Generic top-level domain
- .NF country-code Norfolk Island
- .NG country-code Nigeria
- .NI country-code Nicaragua
- .NL country-code Netherlands
- .NO country-code Norway
- .NP country-code Nepal
- .NR country-code Nauru
- .NU country-code Niue
- Internet Users Society - Niue
- .NZ country-code New Zealand
- .OM country-code Oman
- .ORG generic Generic top-level domain
- .PA country-code Panama
- .PE country-code Peru
- .PF country-code French Polynesia
- .PG country-code Papua New Guinea
- .PH country-code Philippines
- .PK country-code Pakistan
- .PL country-code Poland
- .PM country-code Saint Pierre and Miquelon
- .PN country-code Pitcairn
- .PR country-code Puerto Rico
- .PRO generic-restricted Restricted to credentialed professionals and related entities
- .PS country-code Palestinian Territory, Occupied
- .PT country-code Portugal
- .PW country-code Palau
- .PY country-code Paraguay
- .QA country-code Qatar
- .RE country-code Reunion
- .RO country-code Romania
- .RS country-code Serbia
- .RU country-code Russian Federation
- .RW country-code Rwanda
- .SA country-code Saudi Arabia
- .SB country-code Solomon Islands
- .SC country-code Seychelles
- .SD country-code Sudan
- .SE country-code Sweden
- .SG country-code Singapore
- .SH country-code Saint Helena
- .SI country-code Slovenia
- .SJ country-code Svalbard and Jan Mayen
- .SK country-code Slovakia
- .SL country-code Sierra Leone



Country Extensions-

- .SM country-code San Marino
- .SN country-code Senegal
- .SO country-code Somalia
- .SR country-code Suriname
- .ST country-code Sao Tome and Principe
- .SU country-code Soviet Union (being phased out)
- .SV country-code El Salvador
- .SZ country-code Swaziland
- .TC country-code Turks and Caicos Islands
- .TD country-code Chad
- .TEL sponsored Reserved for businesses and individuals to publish their contact data
- .TF country-code French Southern Territories
- .TG country-code Togo
- .TH country-code Thailand
- .TJ country-code Tajikistan
- .TK country-code Tokelau
- .TL country-code Timor-Leste
- .TM country-code Turkmenistan
- .TN country-code Tunisia
- .TO country-code Tonga
- .TP country-code Portuguese Timor (being phased out)
- .TR country-code Turkey
- .TRAVEL sponsored Reserved for entities whose primary area of activity is in the travel industry
- .TT country-code Trinidad and Tobago
- .TV country-code Tuvalu
- .TW country-code Taiwan
- .TZ country-code Tanzania, United Republic of
- .UA country-code Ukraine
- .UG country-code Uganda
- .UK country-code United Kingdom
- .UM country-code United States Minor Outlying Islands
- .US country-code United States
- .UY country-code Uruguay
- .UZ country-code Uzbekistan
- .VA country-code Holy See (Vatican City State)
- .VC country-code Saint Vincent and the Grenadines
- .VE country-code Venezuela, Bolivarian Republic of
- .VG country-code Virgin Islands, British
- .VI country-code Virgin Islands, U.S.
- .VN country-code Viet Nam
- .VU country-code Vanuatu
- .WF country-code Wallis and Futuna
- .WS country-code Samoa
- .YE country-code Yemen
- .YT country-code Mayotte
- .YU country-code Yugoslavia (being phased out)
- .ZA country-code South Africa
- .ZM country-code Zambia
- .ZW country-code Zimbabwe

What is “phishing”

- In the field of computer security, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by **masquerading** as a trustworthy entity in an electronic communication.



Phishing example - email

- Subject: eBay Account Verification
 - Date: Fri, 20 Jun 2003 07:38:39 -0700
 - From: "eBay" <accounts@ebay.com> Reply-To: accounts@ebay.com
 - To: Dear eBay member,
As part of our continuing commitment to protect your account and to reduce the instance of fraud on our website, we are undertaking a period review of our member accounts. You are requested to visit our site by following the link given below
<http://fraud.ebay.com>
- Please fill in the required information.
This is required for us to continue to offer you a safe and risk free environment to send and receive money online, and maintain the eBay Experience.
Thank you
- Accounts Management As outlined in our User Agreement, eBay will periodically send you information about site changes and enhancements. Visit our Privacy Policy and [User Agreement](#) if you have any questions.

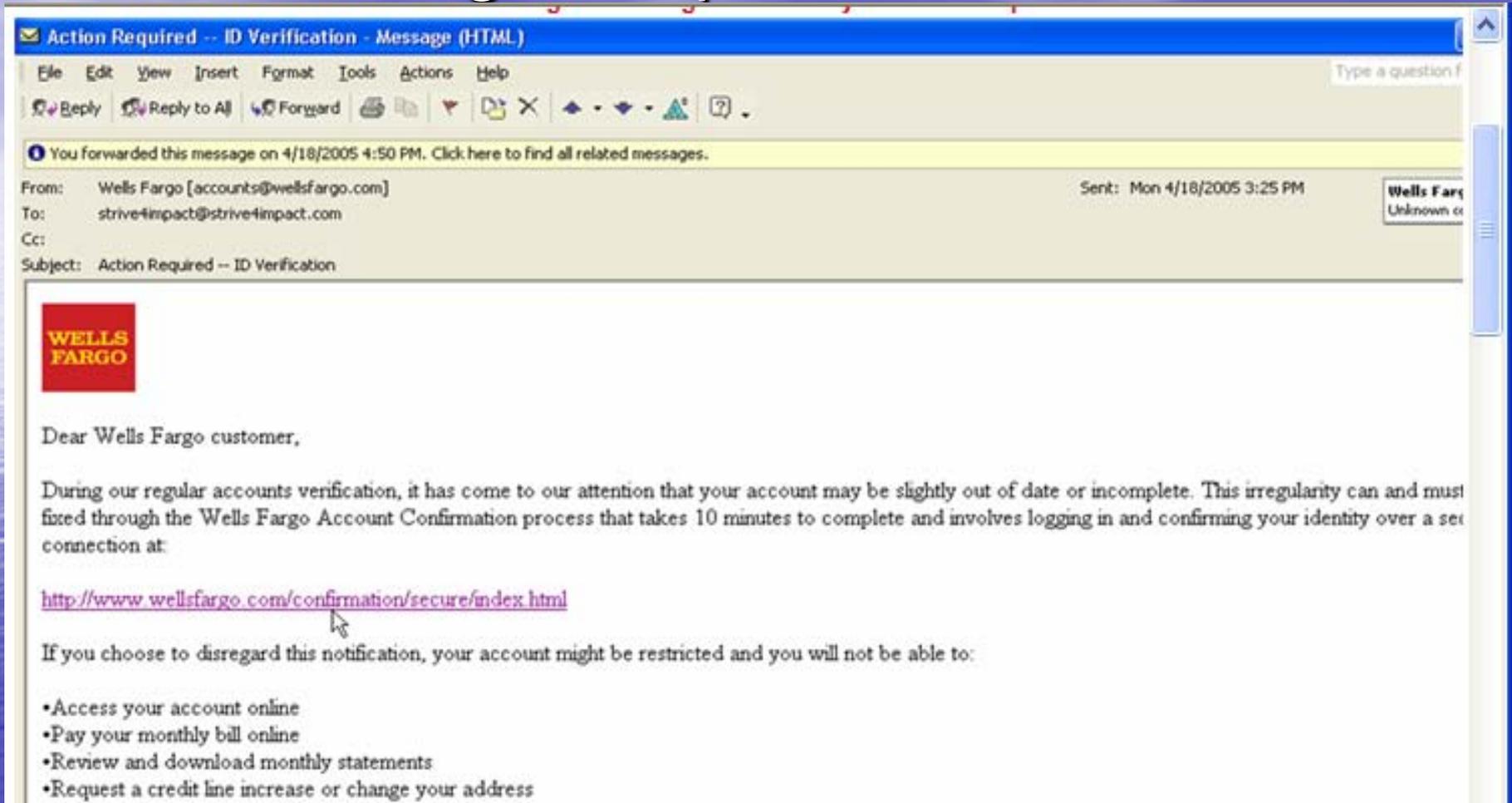


Phishing example - email

- Subject: eBay Account Verification
- Date: Fri, 20 Jun 2003 07:38:39 -0700
- From: "eBay" <accounts@ebay.com> Reply-To: accounts@ebay.com
- To: Dear eBay member,
As part of our continuing commitment to protect your account and to reduce the instance of fraud on our website, we are undertaking a period review of our member accounts. You are requested to visit our site by clicking [HERE](#)

Please fill in the required information.
This is required for us to continue to offer you a safe and risk free environment to send and receive money online, and maintain the eBay Experience.
Thank you
- Accounts Management As outlined in our User Agreement, eBay will periodically send you information about site changes and enhancements. Visit our Privacy Policy and [User Agreement](#) if you have any questions.

Phishing example – Email to Web



The screenshot shows an email client window with a blue title bar that reads "Action Required -- ID Verification - Message (HTML)". Below the title bar is a menu bar with "File", "Edit", "View", "Insert", "Format", "Tools", "Actions", and "Help". A toolbar contains icons for "Reply", "Reply to All", "Forward", and other actions. A yellow notification bar states: "You forwarded this message on 4/18/2005 4:50 PM. Click here to find all related messages." The email header shows: "From: Wells Fargo [accounts@wellsfargo.com]", "To: strive4impact@strive4impact.com", "Cc:", and "Subject: Action Required -- ID Verification". The "Sent" time is "Mon 4/18/2005 3:25 PM". A small "Wells Fargo" logo is visible in the top right corner of the email content area.



Dear Wells Fargo customer,

During our regular accounts verification, it has come to our attention that your account may be slightly out of date or incomplete. This irregularity can and must be fixed through the Wells Fargo Account Confirmation process that takes 10 minutes to complete and involves logging in and confirming your identity over a secure connection at:

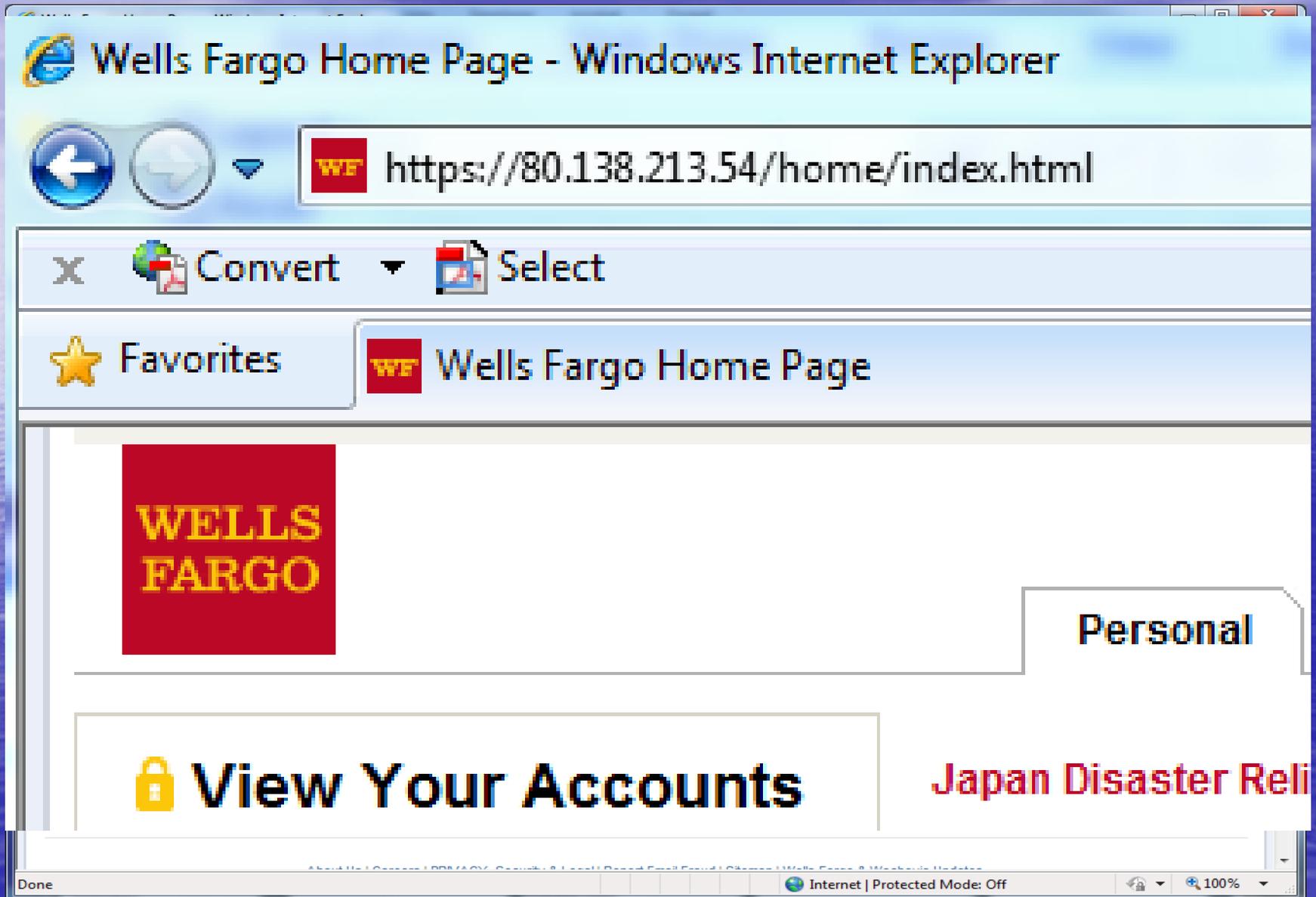
<http://www.wellsfargo.com/confirmation/secure/index.html>

If you choose to disregard this notification, your account might be restricted and you will not be able to:

- Access your account online
- Pay your monthly bill online
- Review and download monthly statements
- Request a credit line increase or change your address

What if I click on this anyway?

What happens if you click?





Phishing example – Email to Web

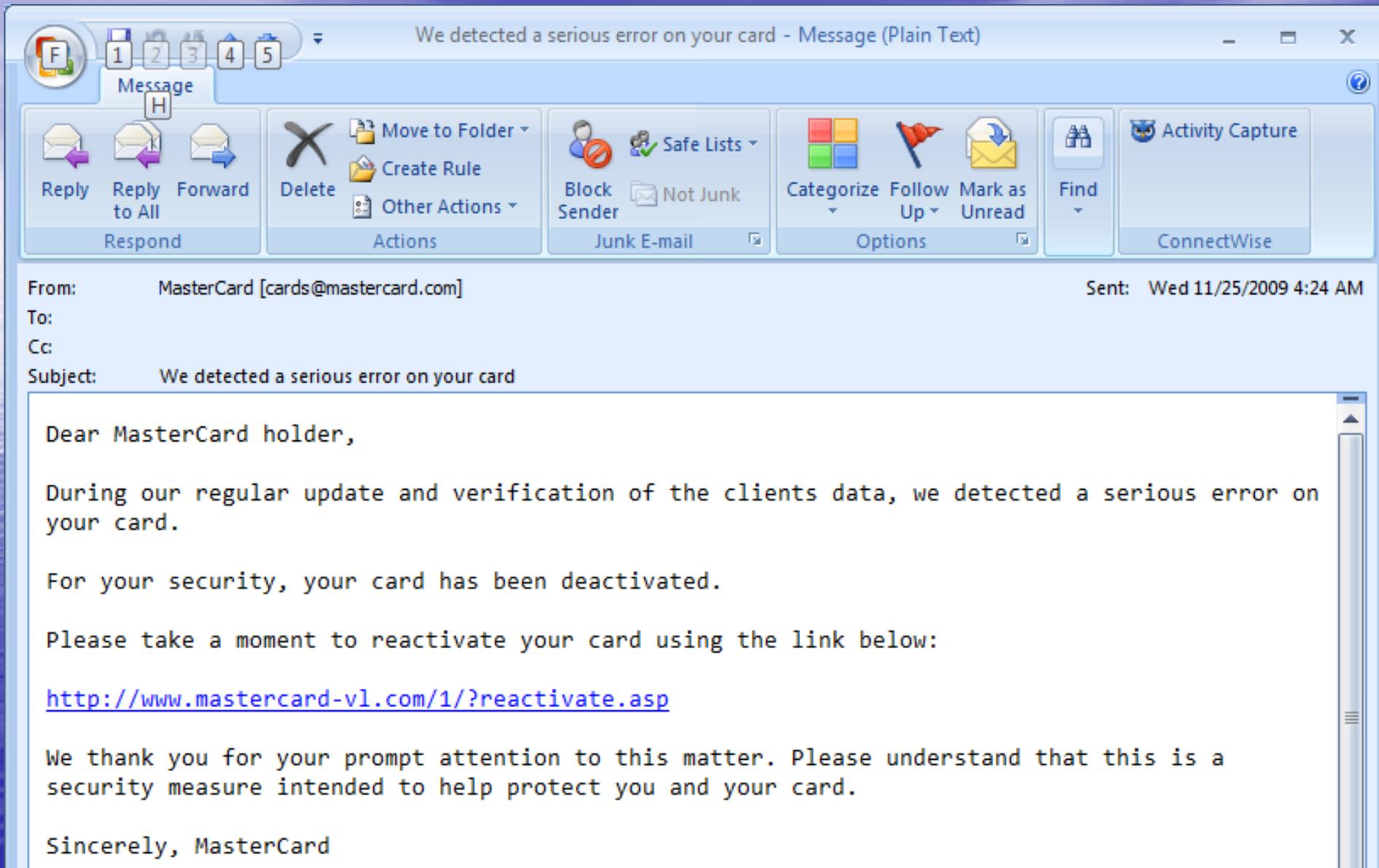
The screenshot shows an email client window titled "for anexeon.com email service user - Message (Plain Text)". The interface includes a toolbar with various actions like Reply, Forward, Delete, Move to Folder, Create Rule, Other Actions, Block Sender, Not Junk, Categorize, Follow Up, Mark as Unread, Find, Related, and Select. The email content is as follows:

Extra line breaks in this message were removed.

From: noreply@anexeon.com Sent: Fri 11/20/2009 4:47 PM
To: Curt Miller
Cc:
Subject: for anexeon.com email service user

Dear owner of the curt@anexeon.com mailbox, You have to change the security mode of your account, from standart to secure. Please change the security mode by using the link below:

<http://accounts.anexeon.com.ftpddrs.be/webmail/settings/noflash.php?mode=standart&id=067842893610824272709639079130847791688292193828131120292&email=curt@anexeon.com>



The screenshot shows an Outlook window titled "We detected a serious error on your card - Message (Plain Text)". The interface includes a ribbon with "Message" selected, and various action buttons like Reply, Forward, Delete, Move to Folder, and Block Sender. The email header shows it is from MasterCard [cards@mastercard.com] sent on Wed 11/25/2009 4:24 AM. The subject is "We detected a serious error on your card".

From: MasterCard [cards@mastercard.com] Sent: Wed 11/25/2009 4:24 AM
To:
Cc:
Subject: We detected a serious error on your card

Dear MasterCard holder,

During our regular update and verification of the clients data, we detected a serious error on your card.

For your security, your card has been deactivated.

Please take a moment to reactivate your card using the link below:

<http://www.mastercard-v1.com/1/?reactivate.asp>

We thank you for your prompt attention to this matter. Please understand that this is a security measure intended to help protect you and your card.

Sincerely, MasterCard



Phishing Test!

- <http://www.sonicwall.com/phishing/>



Viruses and Trojans

- With most commercial email virus protection systems you are protected from viruses entering via email.
- You are NOT protected when you are surfing and click on things you shouldn't click on!

What is a virus?

- A computer virus is a small program written to alter the way a computer operates, without the permission or knowledge of the user. A virus must meet two criteria:
 - It must **execute** itself. It often places its own code in the path of execution of another program.
 - It must **replicate** itself. For example, it may replace other executable files with a copy of the virus infected file. Viruses can infect desktop computers and network servers alike.

What is a trojan?

- Trojan horses are impostors—files that claim to be something desirable but, in fact, are malicious.
- Trojans usually come packaged in software downloads that seem like they would be useful – like “speeding up your internet” or “toolbars” or games.
 - A very important distinction between Trojan horse programs and true viruses is that they **do not replicate themselves**. Trojan horses contain malicious code that when triggered cause loss, or even theft, of data.
 - For a Trojan horse to spread, you must invite these programs onto your computers; for example, by opening an email attachment or downloading and running a file from the Internet.

Windows Security Center

Security Center
Help protect your PC

Resources

- Get more security support details through the Information Center.
- Check your system now for the latest spyware threats & infections.
- Get the latest security and virus information from Microsoft.
- Keep your system protected from spyware, adware and threats.

Security Information: What is Spyware?

Spyware is a computer software developed to intercept or take control over your interaction with your computer. It gets installed without your consent or knowledge and it can monitor your online behavior or even send out your personal information to the developers of the software.

[Install a suitable AntiSpyware Protection for your system.](#)

Advanced XP Defender OFF

Advanced XP Defender is a powerful mix of Anti-Malware, Anti-Virus, Anti-Trojan, Anti-Backdoor, Anti-Worm and Anti-PornoDial in one program. It will protect you from all types of Viruses on your PC.

[Remove threats](#) [Install now](#)

Ultimate Defender OFF

Detect and remove viruses, worms and trojans at once. Keep your files safe from Internet Threats. Protect your privacy by detecting and cleaning spywares and blocking their activities of identity theft automatically.

[Free scan now](#) [Install now](#)

Advanced XP Fixer OFF

Advanced XP Fixer is a powerful mix of Anti-Malware, Anti-Virus, Anti-Trojan, Anti-Backdoor, Anti-Worm and Anti-PornoDial in one program. It will protect you from all types of Viruses on your PC.

[Features](#) [Install now](#)

Manage security settings for:

- [Internet settings](#)
- [Automatic updates](#)
- [Windows firewall](#)

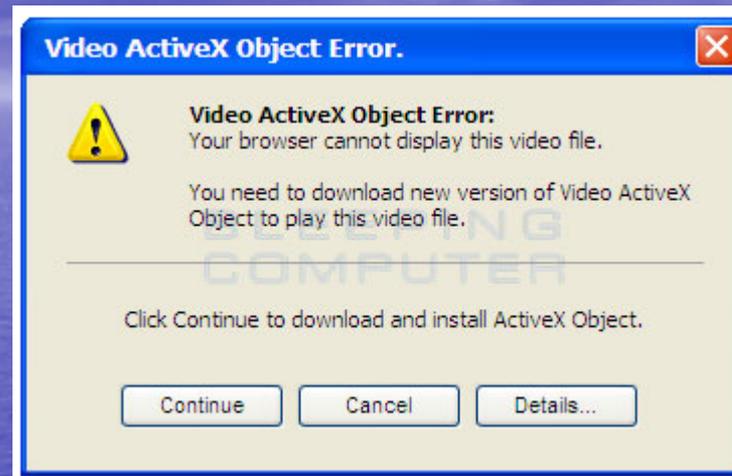
We care about your privacy. Please read our [privacy statement](#).



Why are they more dangerous?

- Trojans are nearly impossible to protect against because they are purposely downloaded by the user and installed.
- An example is a "game" or toolbar that actually instead erases your hard drive.

Trojan Examples



Dangerous links!

Shareware.com - Search for shareware programs and free software downloads. - Windows Internet Explorer

http://www.shareware.com/

shareware downloads

MailFoundry

Shareware.com - Search ...

SHAREWARE.com
search for shareware programs & free software

Tuesday, July 21, 2009

Ad Feedback

 **Recommended Download**

Editor's Rating: ★★★★★ Rated 5 Stars by Brothersoft (May 2009)

Operating System: Windows 2000/XP/Vista

DOWNLOAD HERE!

THIS WEEK'S TOP SEARCHES: [Spybot](#) | [Ad-aware](#) | [WinRAR](#) | [WinZip](#) | [Winamp](#) | [Spyware](#)

All Platforms **SEARCH**

SPONSORED DOWNLOADS

sponsored

Dashboard Software

NEWEST TITLES

Internet 100%

Summary

- No financial institution will EVER solicit you to "update" passwords, usernames or personal information via email.
- Avoid clicking on ANY link to download software unless you are on a known, trusted site (look at the domain name)
- If it looks suspicious or you are not sure – DON'T CLICK!



Thank You

- Questions???